



SECURE YOUR WIFI NETWORK

Running an unsecured wireless network compromises your computer's security and puts you at risk. Karl Wright shows you how to make your network as safe as houses

In July 2005, Londoner Gregory Straszkiwicz was convicted of repeatedly using his neighbour's WiFi connection, fined £500 and given a 12-month suspended sentence. He may be unique in having the misfortune of getting caught, but Straszkiwicz is not the only one stealing his neighbour's bandwidth. According to a survey carried out last year by AOL, nearly one in six UK computer users (six per cent of women and 22 per cent of men) admit to having illicitly used someone else's wireless broadband connection.

None of this should come as a big surprise to anyone. Take your notebook down a residential street in any British town or city, and the chances are you'll discover at least one unsecured wireless network along the way. In a study carried out last year, the computer security company Panda Software found that up to 60 per cent of users did not secure their network. One reason why people don't take wireless security seriously is that they don't appreciate the dangers they are facing. Allowing unauthorised access to your network and to your broadband connection can have serious and potentially far-reaching consequences.

In this article, we will explain how you can secure your wireless network. We'll walk you through the basic steps you can take to restrict

access, right up to the advanced data-encryption techniques used in major enterprises.

KNOW YOUR ENEMY

In the most benign scenario, a hacker will, like Straszkiwicz, just steal your bandwidth. This may sound trivial, but it could soon become intensely annoying. If, for example, the hacker is using bandwidth-intensive applications such as P2P file-sharing, you may experience a very slow internet connection.

A more mischievous intruder could easily use an unsecured wireless network to access the computers on your network. Once they have access to your network, it's easy for the intruder to steal your data. In 2004, Brian Salcedo of North Carolina was convicted of stealing credit card information from a chain of hardware stores. He did this by logging on to an unprotected WiFi access point and installing a program that monitored card numbers being entered into the store's database. While your home PC might not contain a list of customer credit cards, someone could gain access to your private correspondence, your PayPal user login details and your online banking records.

Then there's drive-by pharming. This is a relatively recent phenomenon whereby a hacker sets up a webpage with some hidden code that

will make significant changes to the configuration of your broadband router or wireless access point, without you having to download anything. These changes mean that its DNS server settings will point to the hacker's DNS server. The hacker has control of your internet connection and can send you to whichever site they want you to go to, regardless of the address you entered. This type of attack is successful because many people don't change the default password on their router, making it easy to guess.

In the final and most disturbing scenario, an intruder who gains unauthorised access to your wireless network could use your PC and your broadband connection to break the law. They might use your connection to download child pornography, illegally share copyrighted material or upload viruses and other forms of malware to the internet. They might even use your network connection to commit a serious hack. One of the ways in which hackers make it difficult for others to trace them is by remotely taking over the PC of an unsuspecting victim and then using that PC to perpetrate a crime. When the hack is traced, initially at least it will be traced back to the IP address of the first victim. But this method has drawbacks: it can be difficult to execute, and it may put the



Drawing the curtain Wireless networking and Windows Vista

In Windows Vista, the way in which you connect to wireless networks has been simplified. Rather than right-clicking in the taskbar (though this is still possible) the new user simply has to choose Connect to from the Windows Vista Start menu. This opens the 'Connect to a network dialog' box, which is basically a redesigned version of the 'Choose a wireless network' dialog box from Windows XP. In the drop-down menu at the top of the dialog box, you can choose to show all networks, wireless networks only, or dial-up and virtual private networks only. See page 138 for details of how to secure your wireless network with a VPN.

Unlike the wireless networking tool in Windows XP, Vista can see and display wireless networks that don't broadcast their identifying names (their SSIDs). Windows Vista also allows you to set this kind of 'hidden' wireless network as your default wireless network, to which Windows connects automatically every time you boot your PC. Windows XP can't do this. If there is a named wireless network in the vicinity, it will always try to connect to that network first.

If the network to which you wish to connect is listed, click on it and enter the WPA security key. If it isn't listed, click on the 'Set up a connection or network' option. On the next

screen, choose to set up a wireless, broadband or dial-up connection. Hereafter just follow the wizard, entering the SSID of the desired network along with the encryption key, then click Connect.

Right-clicking the wireless network icon in Windows Vista also reveals a broader range of options than those available in Windows XP. You can turn off the pop-up windows that tell you a new wireless network has been found (a source of irritation in Windows XP with Service Pack 2) and you can open the Network and Sharing Center, which is the Vista equivalent of Windows XP's My Network Places.

authorities off the scent for a short time only. Connecting to an unsecured wireless network, however, is easy, and unless the victim has enabled connection logging on their router (which is pretty unlikely) it will probably leave no traces.

At this point, you may be feeling complacent, safe in the knowledge that you have already activated at least some of the security features on your wireless router. But don't relax too soon. Many of the security features on which people rely, such as hiding their network's name or restricting access by MAC address, can be overcome.

Hackers who specialise in gaining unauthorised access to wireless networks are known as wardrivers. Their technique is simple. With his or her computer discreetly tucked away in a backpack, the wardriver takes a leisurely stroll around a neighbourhood. As they walk, the computer is busy logging details of each wireless network it discovers, including the GPS coordinates at which the network can be found.

Once the wardriver gets home, the information gathered is examined, the most vulnerable networks are identified and their locations pinpointed using the GPS coordinates. It is possible to feed the log from one of these wireless sniffing programs into Google Earth to build 3D maps showing where vulnerable networks can be found. Once a target is chosen, the hacker returns to the location, sits or parks

somewhere in the vicinity and gets to work on cracking the network.

CHANGING PASSWORDS

The first thing you should do when you set up your wireless network, even before you give the network a name, is change your router's default password. If you don't do this, anyone who logs on to your network will be able to reconfigure your router. This doesn't just mean hackers, but also hapless spouses, mischievous children or house guests. As well as changing your router's default username and password, you should also give your network a name. In many cases a wireless network's default name, referred to as its service set identifier (SSID), is the router's own model name. A would-be hacker can use this information, searching online for known security flaws in your hardware.

Many wireless security guides also advise you to hide your network's name. This is easily done. Simply open the router's presentation page and select the setting that says 'Disable SSID broadcast' or something similar. Only wireless networks with an SSID are listed in the Windows XP Choose a wireless connection dialog box, so most of your neighbours won't even know that your network is there. They might still be able to find the network, but a connection could be made only if the SSID were known. You, however, can still log on to the network, because you will be able to tell

Windows the network's name before you try to connect.

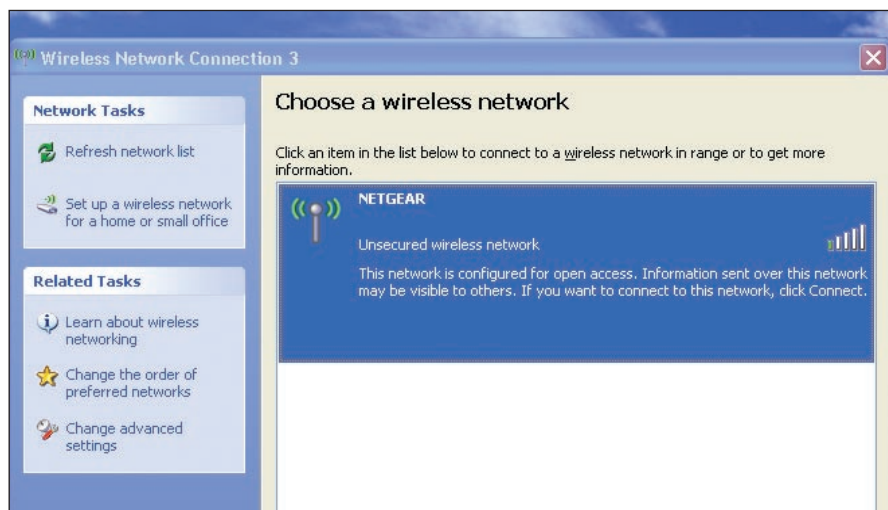
Or so the theory goes. Unfortunately, this thinking is flawed. While the Windows XP network utility doesn't inform its users of networks that don't broadcast their SSID, plenty of freely available WiFi sniffers do; even Windows Vista does, as the box above explains. Once a hacker has found your network, finding out its name is simple. Every time a PC logs on to your network (for instance, when it first boots), it transmits the SSID in clear text as part of its authentication sequence. Even if you use WEP or WPA encryption, the SSID is still transmitted unencrypted as part of the authentication process. All the hacker has to do is intercept these unencrypted packets and he can quickly find out your SSID.

By all means hide your SSID. It pays to use as many different security measures as you can, and anything that makes your network even a little bit harder to hack than your neighbour's is worthwhile. Just don't let hiding your SSID lull you into a false sense of security. You need to implement other, far more stringent security measures as well.

ADDRESS CODE

Each network adaptor on your wireless network is associated with two numbers: its MAC address and its IP address. The MAC address is unique to your network adaptor and never changes. The IP address of each device is automatically assigned by the router (this is referred to as the DHCP function) and need only be unique on your network. Another simple security measure is to configure your router so only known adaptors, those with recognised MAC addresses, can connect to it. You can go one step further and prevent your router automatically assigning IP addresses to new wireless clients. You must then tell the router which IP address it should assign to each recognised MAC address. You need do this only once; then, every time a device using the recognised adaptor logs on, it uses the IP address you have specified. If an unknown adaptor tries to connect, the router simply refuses the connection attempt.

Again, while this is great in theory, it is quite easy for a hacker to discover and 'spoof' (imitate) authorised MAC addresses and IP addresses. It is worth limiting access by MAC address and preventing your router dynamically assigning IP addresses, but only as part of your overall security. Such measures are no substitute for having a properly encrypted network.



▲ We happened across this network belonging to a neighbour. It's unsecured, and because the UPnP protocol is enabled, the router also appeared under Network Connections as a UPnP device. Had we been so inclined, we could have opened this network's presentation page and changed any settings we liked

NETWORK ENCRYPTION

Once all your basic security measures are in place, the next step is to encrypt your network properly. This is by far the most common form of network security. When done properly, it will deter all but the most knowledgeable and determined of hackers and, along with the measures covered previously, it should suffice for most home users.

When wireless first came on to the market, the standard encryption scheme was Wired Equivalent Privacy (WEP). As its name suggests, WEP was supposed to make your wireless network as secure as a wired network. Unfortunately, it didn't. WEP suffered several flaws, making it vulnerable to a patient hacker. For this reason, we do not recommend that you rely on WEP encryption unless you have absolutely no choice. Thanks to firmware updates, even older hardware now tends to support the newer WPA encryption standard. The only exceptions we have seen recently are some older wireless print servers, which still support only WEP. If you simply must use WEP, because one of your devices doesn't support WPA, we suggest using not only MAC and IP filtering but also a virtual private network (VPN). See the 'Advanced security options' section and the walkthrough on page 138.

WEP supports two types of key: 64-bit and 128-bit. A 128-bit key provides maximum security. Some routers allow you to enter a simple password and use that password to create a WEP key. Others, however, require you to enter a WEP key composed of hexadecimal



◀ Because your wireless network is potentially insecure, your computer's connection to the network should be almost as secure as its connection to the internet. This is why you need a personal firewall on your PC as well as the firewall on your router

numbers manually. Rather than being based on 10 unique characters like decimal numbers, hexadecimal numbers are based on 16 characters – the numbers 0 to 9 and the letters A to F. When you use 64-bit encryption, your WEP key must be 10 characters long, such as 6a413e5048. To use the stronger 128-bit encryption, however, you have to specify a 26-character key.

WiFi Protected Access (WPA) is the replacement for WEP. In WPA, the worst security flaws of WEP have been corrected. It is no longer possible for a hacker to alter the payload of a packet without this alteration showing up in the packet's checksum. Thanks

to the TKIP security protocol, the actual key used to encrypt your wireless data (which is based on a master key specified by the user) is changed every 10,000 packets; this is often enough to deny a hacker the time necessary to analyse encrypted packets and decode the master key. From the user's point of view, WPA is also much easier to use because it doesn't require you to enter keys as a hexadecimal value. WPA keys can consist of any possible combination of numbers and lower- and upper-case letters. In March 2006, the WiFi Alliance announced the release of the WPA2 standard. WPA2 has an even more stringent authentication process than WPA, manages keys

HOW TO... Encrypt your network with WPA

Encrypting your network with WPA is far easier than encrypting with the less-secure WEP protocol. To begin, type your router's IP address into the address bar of your internet browser. This will open the router's presentation page.

1 Navigate to the wireless security section of your router's presentation page and choose the method of encryption that you would like to use. Some routers label these plainly as WEP, WPA with TKIP and WPA with AES. This router doesn't mention WPA, but don't be confused; both the TKIP and AES settings refer to WPA encryption. If your hardware supports it, we suggest that you use the stronger AES standard. Unfortunately, not all the adaptors

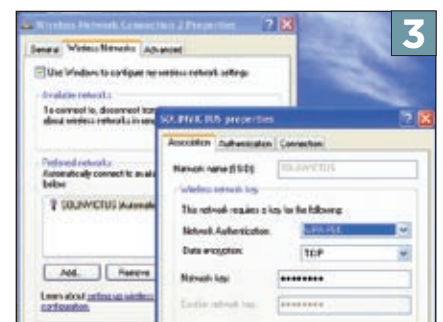
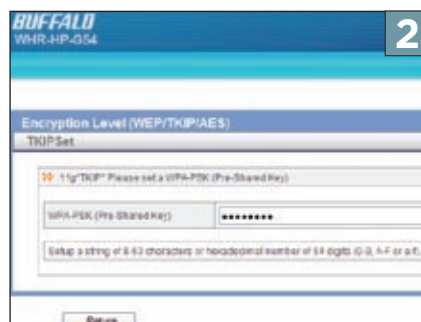
on our network support AES encryption and you can't mix different encryption standards on the same network, so we shall use TKIP.

2 Now you must enter your pre-shared key. By pre-shared, we mean that the individuals who configure the network clients must know this key before they can connect as it will not be generated for them in any way. As you are configuring your own clients, this won't be a problem.

Choose a key that you will be able to remember but others won't easily be able to guess; avoid the name of your partner, pets or children. Try to use both upper- and lower-case letters and numbers. When you've entered the

key, press Apply and your router will restart and then use the new setting.

3 On a client PC that you wish to connect, double-click the wireless network icon in the Windows taskbar. If your wireless router broadcasts its SSID, it will be displayed in the list of networks found. Double-click your network, enter your key and your PC will connect to the wireless network. If your network's SSID is hidden, click on Change advanced settings on the left-hand side. On the Wireless Network tab of the Wireless Network Connection Properties box, click Add and enter the name, encryption type and key for your wireless network. Click OK and your PC should connect to your network.





in a more sophisticated manner and includes a stronger encryption protocol.

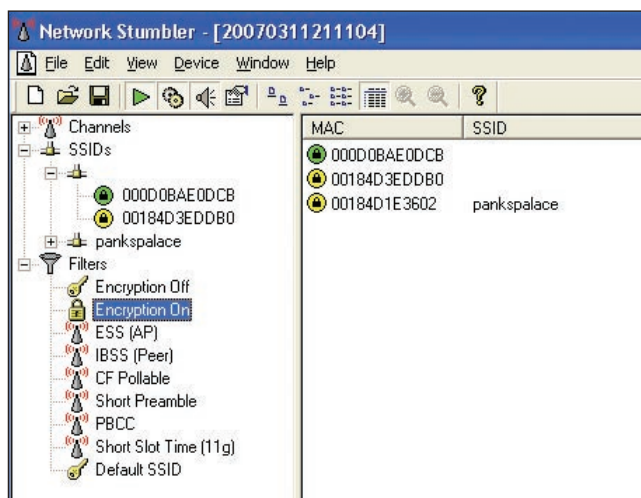
Most routers have a built-in firewall. It pays to make sure that you know how to use yours. As well as activating your router's firewall, each PC on your network should also be protected by a firewall. If a hacker did manage to break into your wireless network, a good firewall program might still prevent him or her gaining access to your PC.

ADVANCED SECURITY OPTIONS

For most users, hiding the SSID, restricting access to known MAC addresses, disabling the DHCP function and encrypting the network with WPA or WPA2 should be sufficient. But if you need even greater security, you could consider setting up a virtual private network (VPN).

VPNs were originally developed to allow computers to communicate as securely over the internet as they would over a private connection. There are two types of VPN: those that use the PPTP protocol, and those that use the more secure L2TP over IPSec. The former is easier to configure, but if you really need an extra level of security, you should take the time to create a VPN that uses L2TP over IPSec.

The best way for a home user to set up a VPN is by using a VPN-capable router. Some caution is necessary; many routers claim to be VPN-compatible, but on closer inspection it turns out they have only a 'VPN pass-through' capability. This means they are able to route VPN packets to their correct destination, but they cannot act as a VPN server. If you wish to secure your wireless network using a VPN, you'll need a router capable of acting as a VPN server. We show you how to secure your wireless network using a VPN in the walkthrough below.



◀ The owner of the Netgear router we looked at previously (see page 136) had hidden their SSID a few days later (we could only find their network using the program Netstumbler) and had encrypted their network with WPA. Their neighbours can no longer steal Netgear's bandwidth or mischievously reconfigure the router

The only drawback with using a VPN is that you have to connect to it every time you want to use your wireless network, which undermines the convenience of having a broadband connection. We recommend this measure only to those who have genuine and well-grounded fears for the security of their network.

OTHER CONSIDERATIONS

As well as implementing sophisticated encryption and access control, there are some simple steps you can take to make your network more secure. One of the most simple but effective is to place your router in the middle of your house rather than close to an outside wall. This will reduce the chance of your network being broadcast into the street. If a hacker can't get a strong enough signal to log on, they will not be able to compromise your network. Some routers also allow you to adjust the strength of

your wireless signal, which is a more sophisticated way of achieving the same effect. You could also consider turning off your network if you know you won't be using it for an extended period. Previously this wasn't advisable because some older routers used to lose their settings when they were turned off. Thankfully, we haven't seen this problem for some time.

If you use all the security measures in this article, your wireless network will be as secure as it possibly can be. It might still be theoretically possible to circumvent your defences, but unless you have the secret of alchemy or the whereabouts of Osama bin Laden stored on your PC, it's going to be far too difficult to be worth anyone's while. It sounds cynical, but to a large degree this is the key to wireless security: making life so difficult for the prospective hacker that they will just go somewhere else and look for a network that's less well defended. **CS**

HOW TO...

Secure your wireless network with a VPN

In this walkthrough, we'll show you how to use the built-in Windows VPN client and Draytek's Vigor 2600VG router to secure your wireless network with a VPN.

The steps are almost identical to those you would take if you were setting up a VPN to which users could connect over the internet. The only difference is that you must make sure the IP address of your VPN is the router's local IP address. Once you have set up your VPN, you need to connect to it before you can use your wireless network.

1 Open the router's VPN setup page in a web browser and create a user account. Type in a username and password and enable the necessary VPN protocols. You will also need to specify the VPN's pre-shared key. If you use PPTP you won't need to specify a key, but your VPN security won't be as tight.

2 Configure the router to allow access only to PCs with the specified MAC addresses and to require a VPN connection. You should also specify the IP address to which VPN traffic

should be routed: in this case, the router's main public IP address. Specify the right IP address, or your VPN won't work.

3 To set up the client PC, open Network Connections in the Control Panel. Click through to 'Connect to the network at my workplace'. Choose to set up a virtual private network. Give your connection a name and enter your VPN's IP address. Your VPN connection should now appear under Network Connections. Double-click it to connect.

